



FortiAnalyzer

Admin and System Events Report

Report Date: 2013-10-19

Data Range: 2013-10-12 00:00 - 2013-10-18 23:59 CEST (FAZ local)



Table of Contents

Admin and System Event Report	1
Admin Login Summary	1
System Active Summary	1

Admin and System Event Report

Admin Login Summary

Date/Time	User Name	Login Interface	Duration	Config Change	Device	Date/Time	User Name	Login Interface	Duration	Config Change	Device
10/18 05:10	admin		1m 27s	✓	alsochlu-sg0e2	10/17 01:10	admin		6m 37s	✓	alsochlu-sg0e1
10/18 05:10	admin		49s	✗	alsochlu-sg0e2	10/17 01:10	FMG-Admin-al		1m 30s	✗	alsochlu-sg0e2
10/18 05:10	admin		25s	✗	alsochlu-sg0e2	10/17 01:10	FMG-Admin-al		1m 53s	✓	alsochlu-sg0e2
10/18 04:10	admin		52s	✗	alsochlu-sg0e2	10/17 01:10	FMG-Admin-al		25s	✗	alsochlu-sg0e1
10/18 04:10	admin		25m 17s	✓	alsochlu-sg0e2	10/16 08:10	admin		1m 5s	✗	alsochlu-sg0e1
10/18 02:10	admin		12m 54s	✓	alsochlu-sg0e2	10/16 08:10	admin		34m 43s	✓	alsochlu-sg0e1
10/18 01:10	admin		21m 56s	✓	alsochlu-sg0e2	10/16 05:10	admin		15m 25s	✗	alsochlu-sg0e1
10/18 12:10	admin		3m 35s	✓	alsochlu-sg0e2	10/16 04:10	admin		15m 50s	✗	alsochlu-sg0e1
10/18 12:10	admin		14m 13s	✓	alsochlu-sg0e2	10/16 04:10	FMG-Admin-al		4m 13s	✓	alsochlu-sg0e1
10/18 12:10	admin		15m 9s	✓	alsochlu-sg0e2	10/15 08:10	admin		21m 12s	✗	alsochlu-sg0e1
10/17 07:10	admin		23m 39s	✗	alsochlu-sg0e1	10/15 08:10	admin		42m 41s	✓	alsochlu-sg0e1
10/17 07:10	admin		8m 1s	✓	alsochlu-sg0e1	10/15 07:10	admin		25m 4s	✓	alsochlu-sg0e1
10/17 06:10	admin		45m 47s	✓	alsochlu-sg0e1	10/15 06:10	admin		1m 52s	✓	alsochlu-sg0e1
10/17 02:10	admin		15m 46s	✓	alsochlu-sg0e2						

System Active Summary

Date/Time	Events	Device	Date/Time	Events	Device
10/18 02:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL tunnel shutdown	alsochlu-sg0e2
10/18 02:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 01:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 01:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 12:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 12:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 11:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 11:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 10:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 10:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 09:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 09:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	The ntp daemon step adjusted time from Fri Oct 18 17:24:	alsochlu-sg0e2	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-cisco:	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-hp:5	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-ibm:5	alsochlu-sg0e2	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-root:5	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-cisco:	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-hp:5	alsochlu-sg0e1	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-ibm:5	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-root:5	alsochlu-sg0e1	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 08:10	Assigns IP address/configuration parameters to the client	alsochlu-sg0e2	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 08:10	Client requests IP address/configuration parameters	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	DHCP statistics	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	DHCP statistics	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	Completed reputation db maintenance	alsochlu-sg0e1	10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	Completed reputation db maintenance	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL alerts	alsochlu-sg0e2

System Active Summary (contd)

Date/Time	Events	Device	Date/Time	Events	Device
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget:bookmarks roospi gr-SSL-V	alsochlu-sg0e1	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget roospi gr-SSL-VPN-VDOM-r	alsochlu-sg0e1	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user roospi gr-SSL-VPN-VDOM-root	alsochlu-sg0e1	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget:bookmarks roospi gr-SSL-V	alsochlu-sg0e2	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget roospi gr-SSL-VPN-VDOM-r	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user roospi gr-SSL-VPN-VDOM-root	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2	10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2	10/18 07:10	SSL new connection	alsochlu-sg0e2

Appendix A

Devices: alsochlu-sg0e0-root